Personal Identity Verification For Federal Employees and Contractors

National Institute of Standards and Technology
Information Technology Laboratory
Computer Security Division
100 Bureau Drive
Gaithersburg, MD 20899-8900

Basis for Requirements

HSPD-12: Policy for a Uniform Identification Standard

Personal Identity Verification Requirements

HSPD-12: Policy for a Uniform Identification Standard

Secure and reliable forms of personal identification:

- Based on sound criteria to verify an individual employee's identity
- Is strongly resistant to fraud, tampering, counterfeiting, and terrorist exploitation
- Personal identity can be rapidly verified electronically
- Identity tokens issued only by providers whose reliability has been established by an official accreditation process

Personal Identity Verification Requirements

- Applicable to all government organizations and contractors
- To be used to grant access to Federally-controlled facilities and logical access to Federally-controlled information systems
- Graduated criteria from least secure to most secure to ensure flexibility in selecting the appropriate security level for each application
- Not applicable to identification associated with national security systems
- To be implemented in a manner that protects citizens' privacy

Personal Identity Verification Requirements

HSPD: Policy for a Uniform Identification Standard

- Departments and agencies shall have a program in place to ensure conformance within 4 months after issuance of FIPS
- Departments and agencies to identify applications important to security that would benefit from conformance to the standard within 6 months after issuance
- Compliance with the Standard is required in applicable Federal applications within 8 months following issuance

Phase I

Personal Identity Verification Standard for Federal Government Employees and Contractors

- Promulgate Federal Information Processing Standard within 6 months

- Establish requirements for:

  - Identity Token (ID Card) Application by Person
  - Identity Source Document Request by Organization
  - Identity Registration and ID Card Issuance by Issuer
  - Access Control (Determined by resource owner)
  - Life Cycle Management

Phase I (Continued)

- Integrated circuit card-based identity token (i.e., ID Card).
- Standard at framework level with minimum mandatory implementation for interoperability specified.
- Basis for specification of issuer accreditation and host system validation requirements .
- Basis for specification of ID card, data base infrastructure, protocols, and interfaces to card.
- Card/token issuance based on I-9 Identity Source Documents, request by government organization, and approval by authorized Federal official.
- Biometric and cryptographic mechanisms.

Phase I (Continued)

Inclusion of Contactless Capability (ISO/IEC 14443)

- Physical Access Control – Permits moving enough people “through the gate” in a unit of time
- ICAO selected contactless technology for the next generation passport ICAO (for traveler authentication)
- Some Government applications are using small numbers of contact cards for physical access
- FICC workgroup on physical access has selected contactless technology

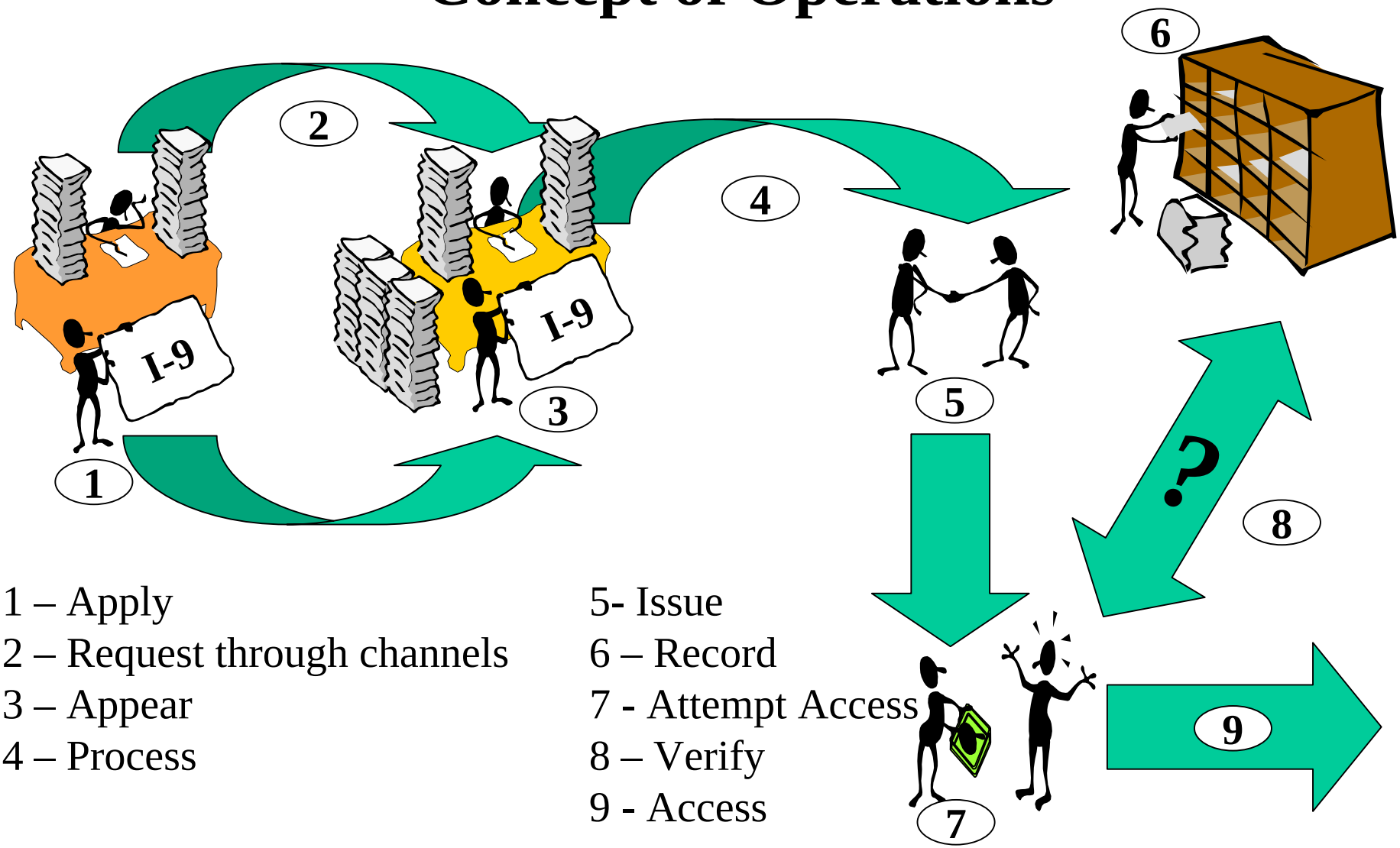
Phase I (Continued)

Inclusion of Biometric Data

- Biometric mechanisms roughly equivalent to a PIN from a security assurance point of view.
- User can't give away, lose, or forget his/her biometric.
- Whether these features significantly improve the security of a given system is open to debate.
- Some experts feel that a card + PIN provides the same assurance level as a card + biometric.

Phase I (Continued)

Concept of Operations



1 – Apply
2 – Request through channels
3 – Appear
4 – Process

5- Issue
6 – Record
7 - Attempt Access
8 – Verify
9 - Access

Phase I (Continued)

Application and Request

- Prospective recipient presents I-9 documents to parent organization
- Parent organization copies I-9 documents and prepares request for identity token
- Parent organization forwards copies of I-9 documents and the request to its management for approval
- Management approves request and forwards copies of I-9 documents and the request to issuing activity (e.g., Security)

Phase I (Continued)

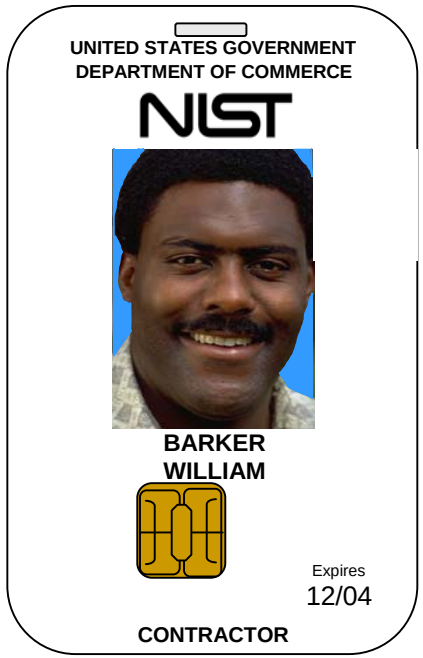
Registration and Issuance

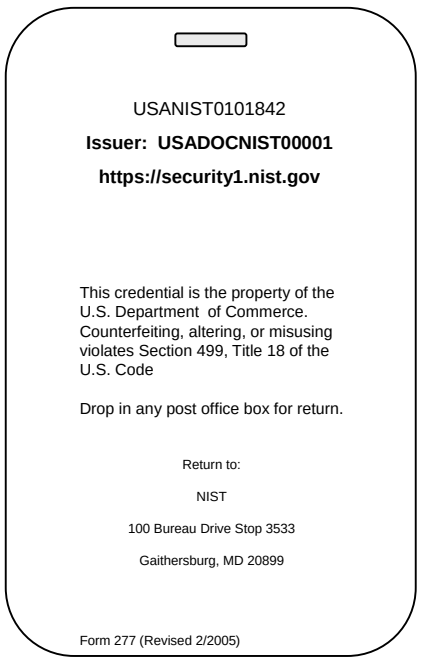
- Issuing organization establishes validity of request.
- Issuing organization verifies that I-9 documents presented by prospective recipient match copies provided by requestor and physical appearance of prospective recipient.
- Issuing organization photographs and fingerprints prospective recipient and has prospective recipient enter a PIN.
- Issuing organization prepares and issues identity token
- Issuing organization enters issuance record into database

Phase I (Continued)

Access Control and Life Cycle Management

- Access control process determined by resource owner.
- Registration databases maintained by issuers as accessible by entities controlling access to resources.
- PKI Certificate management responsibility of issuers.
- Token replaced/re-issued periodically (5 years?).
- Revocation notification for exceptional circumstances (e.g., revocation with prejudice).





Phase I (Continued)

Tentative Mandatory Card Characteristics

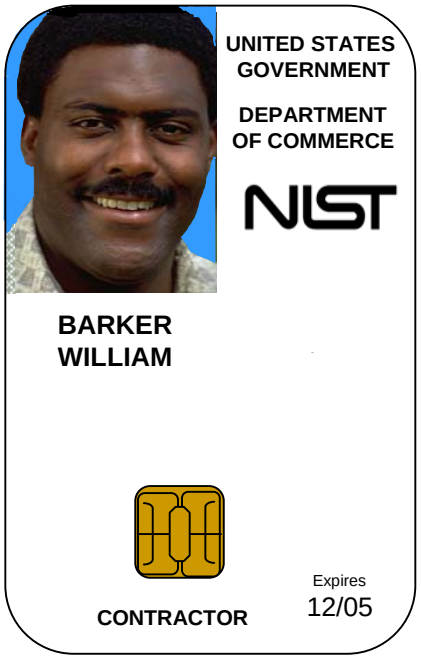
Basic:

- ISO/IEC 7810 Physical Characteristics
- ISO/IEC 7816 (Parts 1-4) Contact Chip
- ISO/IEC 14443 (Parts 1-4 Draft) Proximity Card
- ISO/IEC 24727 (Future) Interoperability Specification [NIST IR 6887]

Mandatory Option Support*:

- 2048 Bit RSA
- 256 Bit AES
- SHA 256
- Fingerprint Image Specification
- Photographic Image Specification

* Illustrative examples only



Phase I (Continued)

Tentative Mandatory Card Content

Electronic Content Digitally Signed By Issuer:

- Digital Photograph (2?)
- Digital Fingerprint Image (Left and right index)
- PKI Certificates (One per access level)
- User Identity (Card number?)
- Issuer Identity

Logic Elements:

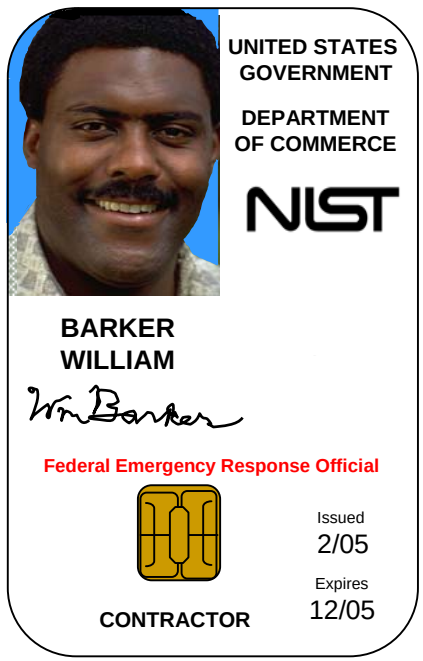
- Cryptographic Digital Signature
- Cryptographic Challenge/Response?
- Encryption/Decryption
- Key Variable Processing (PIN-based notarization?)
- Biometric Data Processing

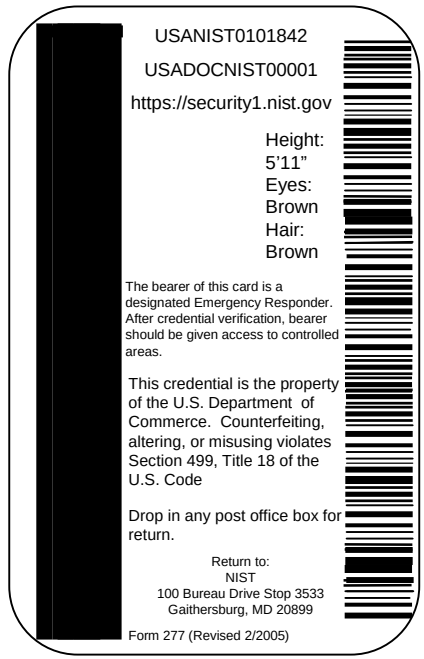
Phase I (Continued)

Optional Card Content

Electronic Content Digitally Signed By Issuer:

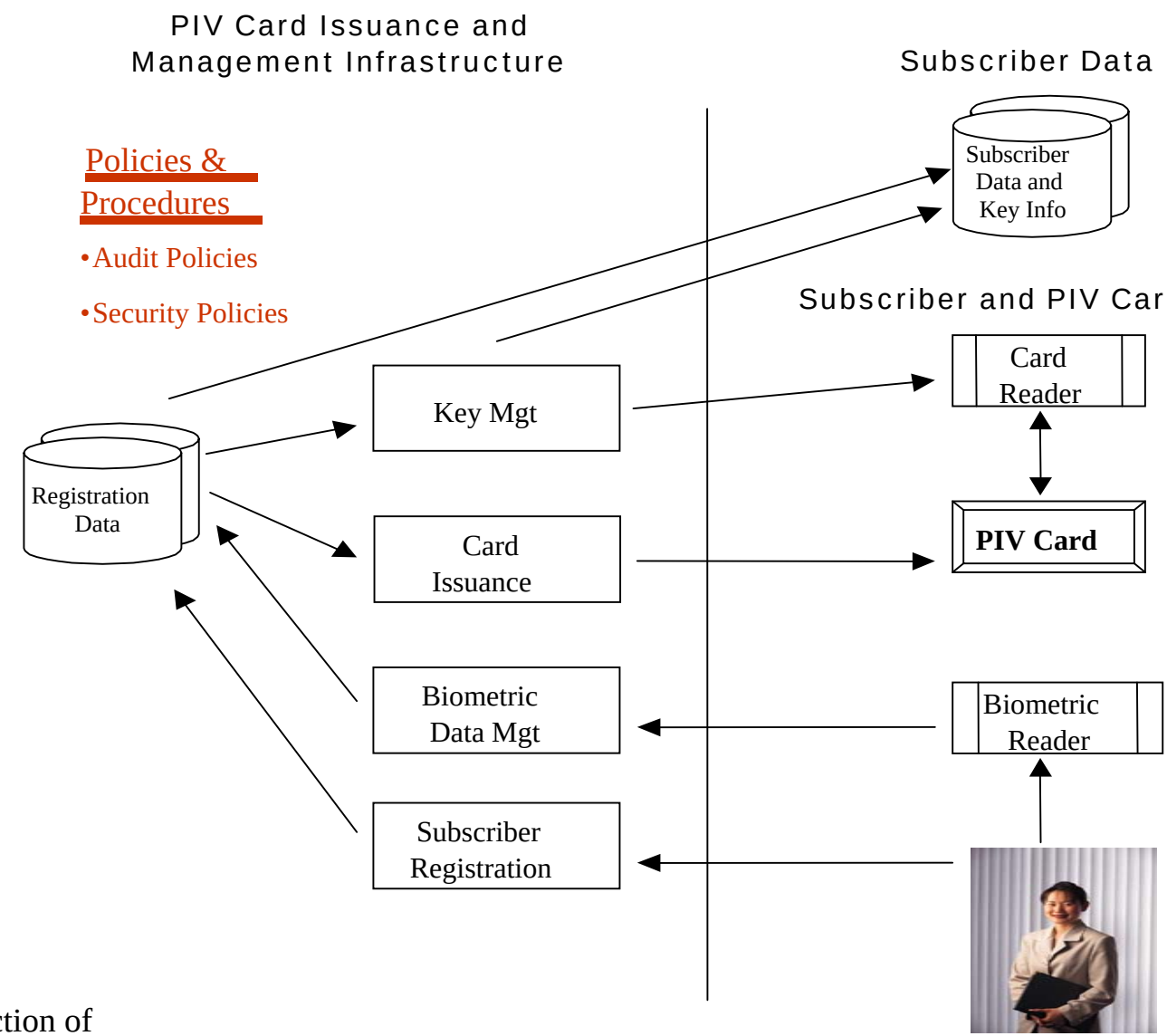
- Employee/Contractor Status
- Second Digital Photograph
- Ten Finger Digital Fingerprint Image
- User's Signature
- Emergency Responder Designation
- Date of Issue
- Height
- Hair Color
- Eye Color





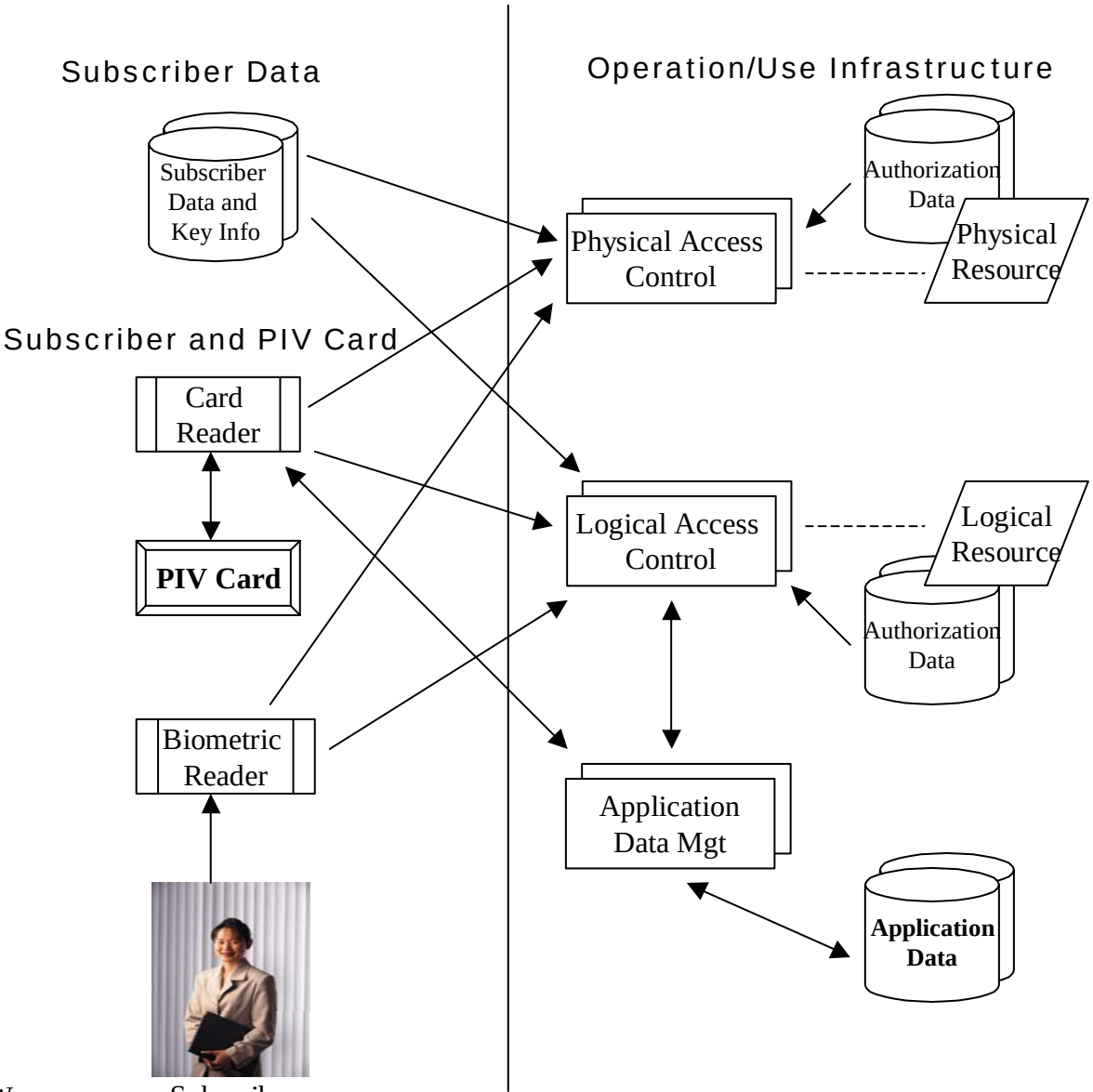
PIV System Concept and Model

PIV Card Issuance and Management

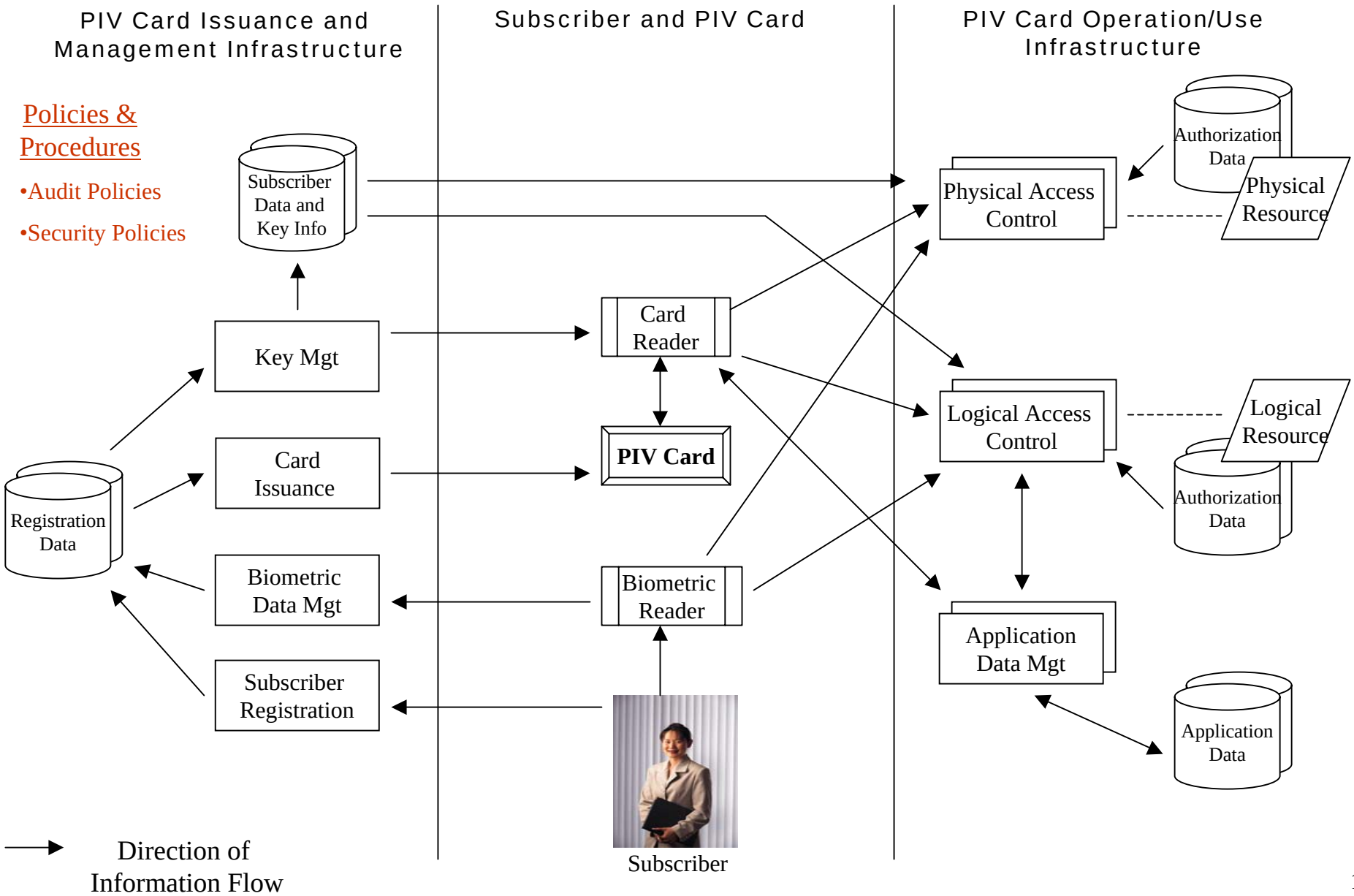


PIV System Concept and Model

PIV Card Operation/Use



PIV System Concept and Model



FIPS Production Plan

Delivery of Detailed Strawman Outline Components -	**August 31, 2004**
Finalize Interagency Working Group Membership -	**September 2, 2004**
Announce First Interagency Working Group Meeting -	**September 2, 2004**
Announce Government Workshop -	**September 3, 2004**
Submit Public Workshop *Federal Register* Announcement -	**September 3, 2004**
Integration Meeting for Concept Draft Components -	**September 3, 2004**
Complete Strawman Content Proposal -	**September 7, 2004**
Distribute Concept to TIWG -	**September 8, 2004**
TIWG Provide Comments to NIST for Review at First TIWG Meeting* -	**September 14, 2004**
First Meeting of Interagency Working Group -	**September 15, 2004**
Collect Initial Draft Component Submissions -	**September 21, 2004**
Completion of Working Group Comment Period -	**September 22, 2004**
Government-only Workshop Day -	**October 6, 2004**
Public Workshop Day -	**October 7, 2004**
Completion of Government Workshop Comment Period -	**October 12, 2004**
Assemble Preliminary Draft -	**October 19, 2004**
Completion of Public Workshop Comment Period -	**October 21, 2004**
Decision on Changes to Draft and Writing Assignments -	**October 22, 2004**
Completion of Public Draft of Standard -	**November 8, 2004**
Completion of Comment Period for Public Draft -	**December 23, 2004**
Completion of Revision of Standard -	**January 13, 2005**
Completion of Responses to Comments on Public Draft -	**January 14, 2005**
Delivery of FIPS Submission Package by NIST to DoC -	**February 4, 2005**
DoC Approval -	**February 25, 2005**

Items on critical path are in boldface.

*** External actions**

Phase I (Concluded)

Consequences of Failure to Accomplish the Task

Non-compliance with the HSPD

- Continued lack of interoperability and mutual acceptance among Federal government badge-based facilities access systems and information system access control systems
- Consequent exposure to penetration of Federal facilities by terrorists and other criminals

Phase II
Implementation-Critical Support

- **Specification of Issuer Software**
  - **Biometrics capture**
  - **Capture, storage, and maintenance of textual information**
  - **Certificate acquisition and management**
  - **Digital signature**
  - **Certificate and cardholder revocation**
  - **PIN capture and use**
  - **Challenge/response programming**
  - **Card data access control**
  - **Issuer data access control**
  - **External interfaces**
- **Management of Software Development and Acquisition (Product by Agency)**
- **Issuer and Component Certification Management (Responsibility/Procedure)**
- **Assignment and Set-up of Inter-agency System Oversight/Management**
- **Coordination of Procurement Specifications (Conformance to Standard)**
- **Set-up and Management/Oversight of Certification Facilities**
- **Logical Access Security Configuration Recommendations/Guidelines (Including Applications)**
- **Establishment of Training Policies/Procedures/Responsibilities/Materials**

Phase II (Continued)

Development and Coordination of Implementing Specifications and Guidelines

- Validation of Requirements and Refinement of Implementation Specification Tasks
- Implementation Standards,Guidelines, Reference Implementations and Conformance Tests
- Security Specifications
- Procurement Guidelines
- Multitechnology Implementation Guidance (to include component placement and physical topology)
- Identity Credential Card Creation and Lifecycle Management
- International Technical Specification Standards
- Secure Communications Protocol Standards

Phase II (Concluded)

Development and Coordination of Standards for Implementing Specifications and Usage Guidelines

Consequences of failure to accomplish Phase II:

- Lack of interoperability among Federal government identity verification activities due to varying implementations of the Standard
- Inability to validate implementations due to absence of conformance criteria and tests
- Potential failure to securely implement the Standard
- Incompatibility of Federal implementations with current and planned foreign government implementations
- Consequent inability to achieve international interoperability